Appl. No. 09 / 993,218
Comm. Dated June 22nd, 2006
Reply To Office action of April 4th, 2006

Remarks / Arguments

Report of the amendments to the claims

-I have amended the first claim #28 to emphasize that the my invention's identity check is a third-party service performed by a genuine third-party examiner host which resides outside of the local network spheres of the client, the client intercepting server (intercepting servers used in Hypponen invention) and the web content source host (web server used in Bates2 invention). I have written further below in the arguments for Hypponen and Bates2 invention a detailed account of the reasons which justify the used particular definition of a third-party computer. I have also emphasized in the claim that the examiner host is a real host as a master server, rather than a subordinate server, such as the Hypponen invention virus scan performing subordinate server. I have also emphasized in the claim that the identity check service has service engagement means which are not used in the prior art, for which details are also provided in the argumentation further below. I have also emphasized in the claim that the identity check relies on the independent identification object in preference over obtaining the web content itself to that identity check (Hypponen and Bates2 inventions both require the presence of the web content itself in the inspection). I have also provided proof that Hypponen invention uses local servers, whether the virus scan server is centralized or not, and that a virus scan is a totally different technology to my invention's identity check, and that Bates2 client requested web content inspection does not need delivering similar identification, neither involves making a similar request, and that Bates2 invention uses only a simplistic database technology.
-I have amended the claims 49 and 50 with a similar amendment like in claim 28, the arguments for claim 28 apply also for these.
-I have canceled the claim 54 and added a new independent claim 55 what focuses on the examiner host.
-I have provided special argumentation for my download information system, claim 45. Examiner's arguments are clearly erroneous, the examiner confuses two fundamentally different technologies: Bates2 virus scan on different e-mails (one per e-mail) to track repeated submissions of virus-infected e-mails, and my invention's renewed updated extra inspection on a one and same already earlier inspected client downloaded web content. See the arguments for claim 45 for more details.
-I have amended the claim 46 and clarified its text.

Preliminary notes about lack of objectivity

I have voluntarily specified my claims further to show the indisputable novelty of my invention. This however does not mean that I accept the arguments of examiner. I have written special protest on page 11 of this paper about the errors in examiner's arguments. The examiner's arguments contain among others the following fundamental errors which I consider most basic-level as it becomes obvious for any reader who is even little technologically cultivated (see more details in the protest argumentation):

Examiner claims that the Hypponen invention virus scan server is a third-party computer

> Wrong! Hypponen figure 1. along with its description clearly points out that their virus scan server is in the same local area network with the client intercepting server and the clients self, whether the virus scan server is used by one or many servers (e.g. also by mail server, proxy server etc.) in the same local area network. See the indisputable facts in detail in the protest argumentation.

-Examiner claims that the Hypponen invention virus scan server is a host computer

Wrong! As the Hypponen disclosure clearly points out, their virus scan server is a subordinate computer in dedicated use of the client intercepting server and possibly other servers in the same local area network. See the indisputable facts in detail in the protest argumentation.

-Examiner claims that the Hypponen invention virus scan server is a remote computer

Wrong! As already noted Hypponen figure 1. with its description leaves no room for misconception, it is in the same local area network with the client intercepting server whether it is centralized (used by multiple servers) or not. See the indisputable facts in detail in the protest argumentation.

-Examiner claims that the Hypponen invention virus scan server performs a remote identity check on web content / file

Wrong! Hypponen only "identifies" if a file is harmful by performing a virus scan on it, this is not identifying a file / web content as defined in my invention. The examiner's claim was most unprofessional and offensively disregarding. See the indisputable facts in detail in the protest argumentation.

-Examiner claims that the Hypponen invention virus scan server performs an identity check in response to a remote service request

Wrong! As already noted Hypponen virus scan server is not a remote computer, and it is not used remotely, and it does not perform an identity check as defined in my invention. It is a subordinate computer to the local servers using it dedicatedly, and the files to be scanned are automatically directed to it; there is no related service request made to the virus scan server, only simple unilateral delivery of the files. See the indisputable facts in detail in the protest argumentation.

As pointed out, the examiner's arguments repeatedly disregard solid facts whether in prior art or in my own invention disclosure. Examiner's arguments are based on wrong personal opinions rather than on evidence-backed demonstration. I have legal right not to accept such flawed examination. The latest arguments of the examiner indisputably point out serious lack of objectivity to do the examination.

I have shown in this and my earlier communication to the Office with undeniable evidence-backed arguments that the examiner: makes no distinction between a subordinate local server and a third-party computer; makes no distinction between a subordinate local server and an independent remote host; makes no distinction between a virus scan and an independent check on web content identifying properties; makes no distinction between processing web content as such and processing only its independent identification; makes no distinction between local and remote identity check; makes no distinction between directing files to a subordinate server, and requesting a service from an independent third-party host. That is against the most basic and fundamental patent examination rules, and violates also prior art conventions for recognizing distinctly different technologies.

The examiner shows disregard to the prior art concepts, prior-art specific disclosure and intended limitations on technological scope, and also to my own invention disclosure, drafted claims and evidence-backed well-reasoned arguments, and to the many discrepancies I have demonstrated to be between examiner's arguments and the prior art as well as my own invention disclosure and drafted claims. I have well-justified reasons to demand better examination quality.

Patentability arguments

Arguments for the first claim #28

Hypponen invention relies on an intercepting local server for inspection, unlike my invention

My invention relies on a third-party examiner host computer in carrying out the crucial part of the inspection, and the amended claim 28 explicitly specifies that the third-party means third-party with respect to the client intercepting intermediate computer (which has interceptive control over client's downloads), as well as the client self and also with respect to the web content source host (which has supply control, and thus de facto interceptive control over client's downloads). I have also explicitly specified in the amended claim that the third-party means the examiner host residing outside of the: local network sphere of the client, local network sphere of the client intercepting server and local network sphere of the web content source host.

The reason why I use the definition "third-party" and not only "remote" for the examiner host in my claims is because my invention technology is designed for the environment where there is no possibility for local direct access to the client requested web content in-situ in its source host, neither in the client intercepting server and neither in the client self. This dilemma is not artificially contrived, such environment has real existence for a remote computer which has to serve clients in diverse localities in the wide area network, when the clients acquire web content from diverse hosts around the wide area network, just as it is the case in my invention. In that environment the inspection performing remote computer cannot reside in the local network sphere of the clients, the client intercepting servers and the web content source hosts. The web content has to be in some way inspected by that remote computer. There are two methods to do that, either transfer the web content to that inspecting remote computer, what is practically impossible and irrational as it would mean enormous waste of network bandwidth and processing time, or use the novel technology of my invention where independent tiny-size identifications of web content are transferred to that remote computer for a special identity check instead.

Thus my definition of third-party computer being third-party with respect to the local network spheres of client, client intercepting server and the web content source host is well-reasoned and justified, because as demonstrated it is an accurate and logically sound description of a novel useful solution for a dilemma which has real existence in a network (traffic) environment which has real existence, as well as an accurate and logically sound description of such network environment itself.

Moreover, my specific definition of a third-party computer is justified also because the client does not acquire web content from the examiner host, neither through the examiner host, in my invention, unlike in Hypponen and Bates2 inventions where the inspection performing servers participate to dissemination and relaying of the web content. The examiner host does not participate to the dissemination and relaying of the web content, neither interferes itself directly with the client internet traffic, so the defined scope is well-reasoned. The useful novel function of the independent third-party processing in my invention is explained more below in arguments for Bates2 invention.

As already noted above earlier with references to Hypponen invention disclosure (fig.1 and its description), Hypponen (US Pub. No. 20030191957) invention relies on an assisting intercepting local virus scan server, which is a subordinate server to local client intercepting servers in the same local network with the client self, in carrying out the inspection for client's downloads. Therefor Hypponen invention is a distinctly different invention.

The amended claim further specifies that my invention's examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server (or such as the

Hypponen invention virus scan server). The amended claim further specifies that my invention's examiner host controls its processes and resources independently, rather than under direct external command.

Besides the claim 28 already specifies that the examiner host computer is a host, and the amended claim emphasizes now that twice, it is a "third-party host computer". Hypponen invention by its design does not need an independent third-party host computer to do the inspection, in fact they do not need any kind of host to perform the inspection, only a subordinate server. A host is recognized by the network computing prior art not merely as a server, but a master server which is not a slave / subordinate server to any other computer in the network. A host is also an independent end-link computer in the network, rather than an automatically data relaying interlink such as Hypponen intercepting servers. Therefor Hypponen invention is a distinctly different invention.

Hypponen invention inspects a file in situ where the file is, not through an independent third-party service which would be separated from the handling of the web content (it would be impossible anyway, because the scan needs the presence of the file); further, the inspection by its design does not need and use any of the service-specific third-party host communication and engagement features of my invention

As already noted, Hypponen invention virus scan server is a local subordinate server, not a third-party host, to the client intercepting server, and the virus scan server both handles the inspected file and performs the inspection for it. The inspection in Hypponen invention is not a third-party service, and the inspection does not involve communicating with a third-party host, or performing even a service request. In my invention the inspection is an independent remote third-party service in separation from the web content handling, and the inspection is performed in response to a special service request, and the inspection involves certain type of service engagement which is specific only to a specialized independent remote third-party host, see the description of the technological details in arguments for Bates2 invention below. Moreover, as the amended claim now clearly says, my invention's identity check relies on the independent identification object in preference over obtaining the web content itself to the identity check, unlike the Hypponen invention which requires the presence of the file itself in the inspection. Moreover, as I have already explained above earlier and in a special protest section of this paper, a virus scan is totally different technology than the identity check of my invention. Therefor the Hypponen invention is a distinctly different invention.

Bates2 invention client specifically requested web content inspection is not a third-party service to the system, neither includes making a similar request, neither includes sending a similar identification when making the request, neither includes similar means of service engagement, neither relies on an identification in preference over obtaining the web content itself to the inspection

In my earlier communication to the Office I mistook the Bates2 (USPN 6,785,732) web server for a local server because of the way it was described in the invention, nevertheless the Bates2 inspections are intentionally done as an integrated process under the direct control of that web server, not by requesting a third-party service. This is the case also when the web server performs the client specifically requested web content inspection in Bates2 invention, the web server is de facto an intercepting server for the web content it provides, not a third-party computer which does not have direct interceptive control over the client requested web content. Moreover, as already noted above, I have further explicitly specified in the amended claim, and the other independent claims, that the third-party computer means third-party also with respect to the web content source host. Quote from the claim: "... a remote third-party host computer in the wide area network, being outside of the local network sphere of: (a) the client computers, (b) any intermediate computer intercepting client requested web content, (c) and, any source host computer of the client requested web content". See the justification of this in the arguments for Hypponen invention earlier above. Therefor the Bates2 invention is a distinctly different invention.

In my invention the independent third-party processing of an independent identification serves an important purpose, it is the only practical and rational architecture in over-the-Internet inspection which is performed on behalf of large numbers of clients which reside in diverse localities in the wide area network, and which acquire web content from diverse hosts scattered around the wide area network. Performing the inspection independently and parallelly in physical separation to the web content handling enables serving multiple clients across the wide area network without causing delays to the clients, and without the clients causing delays to the server itself. Independent third-party processing to carry out the on-demand inspection of an independent identification is an innovative novel feature in my invention. Because of its intelligent mass-service client interaction management, both the processing of the web content and the processing of the inspection becomes much more speedy and effective, and much larger number of clients can be served without the system freezing for overuse. The independent third-party hosting based mass-service architecture also makes possible hereto unseen fast reaction to the emergence of new viruses, as I already have in my earlier communication to the Office demonstrated.

Besides the client made inspection request in Bates2 invention actually concerns the web content itself, there is no specific request to inspect an independent identification. Further, in that Bates2 feature there is obviously no need for a special delivery of an identification which is based on web content properties, and Bates2 does not either show any intention to use delivery of such identification, the invention disclosure is left deficient on that part. A method according to prior art would be a yes/no answer to a simple question whether to inspect the web content, or when it is question of an e-mail message, appointing the specific e-mail with an external list item identifier to be chosen to inspection, not with e-mail message properties.

Moreover, Bates2 invention intends to use a web-mail interface in providing the e-mail service of the web server to its client, as the Bates2 text says (col 5, lines 38-43): "*When a web client that is a registered user of the e-mail server application 124 wants to send an e-mail message, the message is sent from the web browser to the web server that contains the e-mail server application 124, which then sends the message on towards its intended recipient.*". As Bates2 says, the client sent message is sent from a web browser, thus the interface is clearly that of a web-mail, and the same most likely applies to the message reception, the web-mail would be used. In a conventional prior art web-mail interface, any operation (in this case an inspection request) on a specific e-mail message would be made by toggling on a check mark beside the message subject line and pressing a common command button, or pressing a command button beside the message subject line. In code level this means that the message is identified with a simple external list item identifier which has nothing to do with the properties of the e-mail message itself. Other types of web content in Bates2 invention are handled one at a time, for example the client downloading one web page, or one file at a time, and a client specific request concerning inspection for such web content needs only an answer to a simple yes/no question, or pressing a command button in a user interface, to carry out the inspection for the currently handled web content. So the Bates2 client made specific inspection request does not use web content properties to identify the web content chosen for inspection, whatever type web content is inspected. My invention instead purposefully uses special delivery of an independent identification which is based on the web content properties, and it is used to identify web content which is not possessed by the inspection performing computer, unlike in Bates2 invention.

Moreover, as the amended claim now clearly says, my invention's identity check relies on the identification in preference over obtaining the web content itself to the identity check, unlike the Bates2 invention which requires the presence of the web content itself in the inspection. Therefor the Bates2 invention is a distinctly different invention.

Hypponen and Bates2 inventions, like other prior art, do not use special third-party service access technology of my invention

I have further emphasized in the amended claim the role of the examiner host as an independently operating third-party host which has a special way of engagement with its service requestors, by specifying that in response to the identity check service request the examiner host reserves to its service requestor a temporary service-specific: (a) service access, (b) service communication bridge, (c) and, service process. There is no such technology in the examiner referred prior art, because the prior inventions by their intended design have no use for genuine third-party processing to carry out an inspection for an independent identification.

In my invention the examiner host is an independent host with large numbers of clients in diverse localities in the wide area network, which cannot be granted direct control over its service or dedicated connection lines. In this environment, an essential part of the technology is that the examiner host reserves a temporary access, communication bridge and service process for the service requestor (there should be no obscurities that these are part of my invention, my invention specification illustrates in detail that the service is engaged as a temporarily accessed specially requested process performed by an independent host, and a communication bridge is established between the service requestor and the host as described for example in the drawings). The granted access, communication bridge and service process are also service-specific, so there is absolutely no similarity with Hypponen and Bates2 inventions, or other prior art, because they do not need per-inspection specific reservation of a temporary special access, special communication bridge and special process which would yet be means to engage in an independent third-party service. Therefor the Hypponen and Bates2 inventions and other prior art inventions are distinctly different to my invention.

Bates2 invention uses a database, not an independent service of a third-party host

Bates2 invention uses the web server own contained virus information database to check if the source URL-address and links of a web-page or the sender address of an e-mail message are listed as harmful. In a brief description Bates2 says that the virus information database can also be a large centralized database that includes virus information for many web servers, there is however no detailed description or even a drawing about how it would be used in practise, especially no specifying description that it would be anything else than a mere database. In the Disclosure of Invention section of their patent, Bates2 gives only a single introductory description of the database, and it says that the database allows sharing information relating to viruses with other web servers, although it does not specifically mention the centralized database (col 2, lines 47-50). This literally indicates that Bates2 web server own contained database has a role in sharing the database information, wherefor the centralized database would be used only for sharing virus information between the web servers' own databases, not for real-time queries so that it would replace the web servers' own databases. This would fit with the Bates2 disclosure which consistently describes the centralized database only as a database. The conventional prior art method updates databases in larger batches of information in certain time intervals, what is consistent with the Bates2 disclosure where there is no indication to use the centralized database for real-time queries. These are consistent also with the Bates2 absence of specifying disclosure both in text and drawings, what would show the centralized database being a replacement for the web servers' own databases.

Bates2 has very deficient disclosure for their centralized database for that to be considered as a preferred and replacing alternative for the web servers' own databases, and for that to be considered as a complete invention for a person skilled in the art. Still the Bates2 disclosure indicates clearly enough that their centralized database is intended to be only a database which is not used in real-time, and which does not replace the web servers' own databases, but is used only for exchanging updated information with the web servers in larger batches, what is consistent with the prior art practises. Internationally accepted patent examination principles require interpretation against the prior art where the invention disclosure is deficient, like it is in Bates2 invention. I have provided reasonable evidence that Bates2 invention database technology is a totally different technology to my invention where the identity check is performed by an independently operating third-party host computer which is outside of the local network spheres of the source host of the web content, the client intercepting server as well as the client self.

Related Bates2 quotes:

Quote from the Disclosure of Invention introductory invention description, col 2, lines 47-50:
"The preferred embodiments also provide a virus information database that allows sharing information relating to viruses with other web servers and with appropriate authorities, such as law enforcement agencies."

Col 6, lines 6-9:
"Note that virus information database 138 may be a local database, or may be a large centralized database that includes the virus information for many web servers, such as a centralized database that could be accessed via a web site."

<u>Quotes of the amendments in the claim:</u>

Added line: "an examiner host computer, which is a remote third-party host computer in the wide area network, being outside of the local network sphere of: (a) the client computers, (b) any intermediate computer intercepting client requested web content, (c) and, any source host computer of the client requested web content;"

Added line: "wherein the examiner host is an independently operating host as a master server, rather than a subordinate slave server such as a database server;"

Added line: "wherein the examiner host controls its processes and resources independently, rather than under direct external command;"

Added line: "wherein said identity check relies on said identification in preference over obtaining said web content itself to said identity check;"

Added line: "wherein in response to said identity check service request, the examiner host reserves to the service requestor a temporary service-specific: (a) service access, (b) service communication bridge, (c) and, service process;"

Amended line, to literally emphasize that the identification object establishes representation of the identity of the web content in reduced size: "wherein said identification is a data object which is based on certain property(ies) of said web content so that a unique representation of the identity of said web content is established <u>in smaller size</u>;"

Conclusion:
My invention introduces truly independent third-party inspection of an independent identification in separation from the web content handling, the inspection performed by an independent third-party host computer on-demand in response to a special service request, following a service engagement and communication procedure which is specific only to a specialized independent third-party host, unlike the prior art inventions which primarily rely on performing an in-situ

inspection where the web content also is, and which when need a database like Bates2 invention, depend on a direct access interface for using a slave database, and which when need distributed computing like Hypponen invention, unilaterally and automatically deliver the files to be inspected as such by a local subordinate server. As I have thoroughly demonstrated in my argumentation, my invention's independent third-party inspection of an independent identification has an important function in facilitating a novel mass-service and its client interaction management in an environment where large numbers of clients in diverse localities in the wide area network are served remotely on demand without causing disruptions for their Internet traffic which originates from diverse web content hosts around the wide area network. I have also demonstrated that service-specific special engagement and communication with a genuine third-party host when carrying out the inspection is a novel feature in my invention, which is unknown to the prior art. Therefor there is no justification to reject the claim 28 and the related dependent claims.

Arguments for the claim 49

As in claim 28, in the amended claim I have defined the third-party scope of the examiner host more accurately. I have also emphasized the role of the examiner host as independent host and master server. I have also included in the claim the special service engagement features of the examiner host. I have also emphasized that the analysis performed on the identification relies on that identification in preference over obtaining the web content itself to the analysis. See the argumentation for claim 28 for the novelty of these technologies. I have proven in the referred argumentation that these technologies are developed for a special wide area network environment where there exists no comparable prior art solution. Hypponen invention has to do with an environment where the clients exist in a certain specific local network as proven in my argumentation earlier above. Bates2 invention has to do with an environment where clients acquire web content from a certain web server. My invention introduces a novel innovative solution for an environment where the clients in diverse localities in the wide area network acquire web content from diverse hosts around the wide area network. In that environment it is practically impossible to get the web content to a collective inspection which would be performed by a single computer, because of the transfer bandwidth constraints. The key part of the solution is genuine third-party processing on-demand for externally provided independent identifications of web content rather than on web content itself, so that an identification is delivered to an independent third-party host by a computer somewhere along the downloading chain of the pertinent web content.

Conclusion:
I have presented strong evidence of the novelty of my invention in the argumentation of this paper. I have voluntarily made the claim even further highly specified to reflect my invention's novel technologies. Therefor there is no justification to reject the claim 49.

Arguments for the claim 50

As in claim 49, I have made similar amendment by including novel technologies of my invention recited in the amended claim 28. As explained in the argumentation for the claims 28 and 49, these are clearly novel technologies for which there is no prior art.

Conclusion:
I have presented strong evidence of the novelty of my invention in the argumentation of this paper. I have voluntarily made the claim even further highly specified to reflect my invention's novel technologies. Therefor there is no justification to reject the claim 50 and the pertinent dependent claims.

Arguments for the claim 55

I have added the independent claim 55, which includes novel technologies of my invention recited in the amended claim 28. The claim focuses on the examiner host and its role as a third-party host which exists outside of local network spheres of the dissemination source (i.e. a web content host, web server), dissemination route (i.e. client intercepting servers) and dissemination target (i.e. the client) of the web content. The claim also specifies that the on-demand inspection relies on the identification in preference over obtaining the web content itself to the inspection, and that the identification is delivered to the inspection by a computer which is either in the dissemination source, dissemination route or dissemination target of the web content. The claim includes also the special service engagement features of the examiner host and other features recited in the amended claim 28.

Conclusion:
I have presented strong evidence of the novelty of my invention in the argumentation of this paper. I have voluntarily made the claim highly specified to reflect my invention's novel technologies. Therefor there is no justification to reject the claim 55.

Arguments for the download information system, claim 45

Examiner did not review his cited Bates2 feature in relation to my invention carefully enough. Bates2 invention feature of recording the e-mail address of the repeated virus sender comprises performing a virus scan on different e-mails (one scan on each as it is in Bates2 invention), not two inspections in succession on a one and same web content like in my invention. In my download information system it is question of an inspection which is performed anew on a same web content afterwards with more effective / updated inspection. There would be no sense in performing two similar successive inspections on a same web content normally, unless the latter inspection is updated like in my invention.

Bates2 feature is meant for preventing the e-mail submissions of a sender that has a history of sending viruses, protecting the network from such sender (already after the second harmful submission, this has nothing to do with my invention's repeated inspection on a same web content as the examiner claimed). My invention instead is meant to protect web content receiving client itself by tracking its downloads, and by performing later a repeated inspection on an already earlier inspected web content, and by notifying the client if the repeated inspection found the web content as harmful, so that the user of the client computer can take security measures. Bates2 invention tracks the client's submissions and notifies the client if the submissions repeatedly contain a virus. My invention tracks the client's downloads and notifies the client if an already inspected client earlier downloaded web content (which has been given a low security risk status) has been found to be harmful in a renewed inspection on that same web content. Examiner's arguments for my download information system are clearly erroneous, no professional examiner would claim that suppressing a dangerous e-mail sender because of repeated harmful submissions would be the same technology as protecting a web content downloading client with a renewed updated extra inspection on the same web content, whether the web content is e-mail or other type of web content.

Conclusion:
As proven above, the examiner's arguments are flawed, based on misunderstanding and confusing two fundamentally different technologies: Bates2 virus scan on different e-mails (one per e-mail) to track repeated submissions of virus-infected e-mails, and my invention's renewed updated extra inspection on a one and same already earlier inspected client downloaded web content to protect the unsuspecting client. In Bates2 invention the scans serve to track repeatedly harmful submissions, in my invention the download tracking serves to enable renewed inspection on a same web content. So the tracking too has a different function in Bates2 and my inventions. I have presented strong evidence of the novelty of my download information system, therefor there is no justification to reject the related claims 45 and 46.

Protest for misjudgment, invalid premises and continuous inclination to creative re-innovation of prior art in the examination

In the absence of any credible supporting evidence, the examiner has resorted to re-innovating the prior art technologies by inventor-unintended modifications; this conduct is all the more worrying because those distortive re-innovations are further used to claim combinations which do not work, which do not have rational purpose of use, and which are not disclosed in the prior art. A patent examiner's task and responsibility is not to invent new inventor-unintended meanings and uses for the prior art disclosure, but to show enough objectivity to recognize what the prior art says with all the accompanying limitations and technological scope, what is the basic principle of just examination according to the internationally accepted patent examination principles.

I have already in my earlier communication revealed several cases of misjudgment and invalid premises in the examiner's arguments, this same line of disregarding approach towards my invention description and claims, and the prior art disclosure unfortunately continues in the examiner's unjustified arguments. I can show simple examples of insubstantial and invented premises, summing up to multiple instances of illogical reasoning and misconduct in the examination:

Examiner claims that the Hypponen invention virus scan server is a third-party computer

> It is not, as the invention description clearly says it is meant to be a subordinate server for the client intercepting server in the same local area network sphere as the client intercepting server as well as the clients. It is in permanent dedicated use whether used by one or multiple intercepting servers, unlike a third-party computer which is subordinate to no intercepting server, and which is external to the local network sphere, and external to the local system. Hypponen virus scan server is neither external to the local network sphere of the intercepting servers, neither external to the local system. The Hypponen invention drawings, figure 1, also show this clearly, as Hypponen says "*A computer data network (illustrated generally by reference numeral 1) is shown in FIG. 1*", "*All data traffic coming from the Internet 5 to the network 1 passes through the firewall 4a where its access authority is checked.*", "*This virus scanning server 7 is coupled to the network 1 and in use communicates with the protected systems 4 and the administrator's work station 2a.*". As Hypponen clearly says, the virus scanning server (reference number 7) is coupled to the same local network (reference number 1), where the protected systems (client intercepting servers among others, reference numbers 4a-4d) and workstations / clients (reference numbers 2a-2d) also reside, what is clearly shown in the drawing, the local network is enclosed with a sphere and placed below the sphere that describes the Internet. The virus scan server is in the same local network with the client intercepting server whether the virus scan server is centralized (used by multiple servers) or not. The Hypponen final brief note about the "large network" only refers to that same local area network where there is exceptionally large number of local servers in "clusters", and where each virus scan server operates in subordinance to agents / client intercepting servers inside its own cluster (parag. [0042]). It is reprehensible that the examiner acts as if he would not understand this basic-level disclosure in Hypponen invention and the basic-level disclosure in other prior art; I demand reasonably qualified examination which does not distort prior art, and which understands basic concepts of networking technology.

Examiner claims that the Hypponen invention virus scan server is a host computer

> It is not, Hypponen invention virus scan server is not and is not meant to be a host, but an exclusive dedicated servant to the intercepting server(s) as already shown above. My invention's examiner host computer instead is purposefully meant to be an independent host with pertinent communication functions of a host and with novel on-demand service functions of a specialized

host, so the distinction is clear, my invention's examiner host is not a subordinate computer to a server like the virus scan server is in Hypponen invention, but indeed a specialized host.

Examiner claims that the Hypponen invention virus scan server is a remote computer

It is not, as already noted above the figure 1 shows it clearly, so clearly that it is reprehensible to claim otherwisely. Hypponen virus scan server handles and scans client downloaded files as such which requires dedicated always-on high-bandwidth connection with the client intercepting servers. There is no intention and no mention in Hypponen patent text to use the virus scan server remotely, which would be most irrational because of the high-volume traffic between the client intercepting server and the virus scan server. Hypponen self points out the problem of high-volume traffic the virus scan server has to handle by noting that sometimes several virus scan servers has to be employed in the same local network. My invention instead solves among others these kind of bandwidth waste, processing power waste and processing time waste problems in a novel way, what is totally unknown to Hypponen invention.

Examiner claims that the Hypponen invention virus scan server performs remote identity check on web content

It does not, it is not a remote computer as already thoroughly demonstrated above, and it does not perform any identity check on the scanned files; it only scans the files for viruses, there is absolutely no need and intention in Hypponen invention to determine the identity of the scanned files. Examiner claims that checking the file content for a virus is the same as checking the file's identification or identity, what is a most unprofessional and irrational claim. Scanning a file for a virus has nothing to do with determining on the basis of a file's identification if it is already listed as harmful web content. A virus scan determines if the file is harmful by searching virus code from the file, not thus by performing a search for the file's identification in security records to identify the file. A virus scan needs the entire data of a file to be inspected for viruses, whereas identity check as presented in my invention involves using only a small amount of identifying data based on web content properties, such properties being used to establish an independent identification data object for the web content, the identification being transferred elsewhere to a remote examiner host for a special independent inspection against security records. The remarkable distinctions between the technologies are obviously clear even to a novice of the technological field.

Examiner claims that the Hypponen invention virus scan server performs an identity check in response to a remote service request

It does not, it does not perform any identity check, even less the identity check of my invention, as already thoroughly demonstrated above. I have already in my earlier communication to the Office demonstrated that the Hypponen invention virus scan does not require making any kind of service request, because it is performed by a subordinate server to which the client intercepting server automatically directs the files to be scanned, what also comes clearly out of the Hypponen invention description. Hypponen invention virus scan server is a subordinate server which is not requested for services like an independent third-party host is requested for in my invention. The examiner continuously and unprofessionally disregards my well-reasoned arguments which are based on solid facts and evidence by resorting to unprofessional and unethical conduct.

Conclusion:
As demonstrated above and in my earlier communication to the Office, the examination has been repeatedly flawed, wherefor I have the right to demand better examination quality.